CLAIMS

What is claimed is:

1. A method of securely communicating information in a network that includes a host that originates a request, a first server that serves a response to the request, and a second server that cooperates with the first server to respond to the request, the method comprising the computer-implemented steps of:

receiving a first request for a service from the host, which request includes a network address of the host; and

communicating a second service request to the second server based on the first service request and including the host network address only when a first network address of the first server is identical to a second network address of the second server.

2. A method as recited in Claim 1, wherein the request of the host comprises a key value comprising an originating host Internet Protocol (IP) address and a random value.

3. A method as recited in Claim 1, wherein the step of communicating a second service request comprises the step of accepting the host request only when an IP address of the second server is the same as an IP address of the first server.

4. A method as recited in Claim 1, wherein the host is a Web browser and wherein the host request comprises a Universal Resource Locator (URL) that includes an IP address of the host.

5. A method as recited in Claim 1, wherein the host is a Web browser and wherein the host request comprises an HTML POST form that includes an IP address of the host.

6. A method of securely communicating data between a proxy server and a second server, wherein each of the proxy server and the second server are addressable by first

and second Internet Protocol (IP) addresses, respectively, the method comprising the computer-implemented steps of:

receiving, at the proxy server, a first service request from a browser client, wherein the service request includes a third IP address of a client computer associated with the browser client;

communicating a second service request that includes the browser client IP address to the second server only when the first IP address of the proxy server is identical to the second IP address of the second server.

7. A method as recited in Claim 6, wherein the first service request of the browser client comprises a key value comprising the third IP address and a random value.

8. A method as recited in Claim 6, wherein the first service request of the browser client comprises a Universal Resource Locator (URL) that includes an IP address of the host.

9. A method as recited in Claim 6, wherein the first service request of the browser client comprises an HTML POST form that includes an IP address of the host.

10. A method of securely communicating a network address of a client that issues service requests to a first server that proxies the service requests for a second server, comprising the computer-implemented steps of:

receiving a network address of the client;

determining whether a first network address of the first server is equal to a second network address of the second server; and

sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

11. A method as recited in Claim 10, wherein each of the service requests of the browser client comprises a key value comprising an IP address of the client and a random value.

12. A method as recited in Claim 10, wherein each of the service requests of the browser client comprises a Universal Resource Locator (URL) that includes an IP address of the browser client.

13. A method as recited in Claim 10, wherein each of the service requests of the browser client comprises an HTML POST form that includes an IP address of the browser client.

14. A data communications apparatus that securely communicates a service request that is received from a client, comprising a first server that proxies the service request for a second server, the first server comprising means for receiving a network address of the client; means for determining whether a first network address of the first server is equal to a second network address of the second server; and means for sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

15. An apparatus as recited in Claim 14, wherein the service request comprises a key value comprising an IP address of the client and a random value.

16. An apparatus as recited in Claim 14, wherein the service request comprises a Universal Resource Locator (URL) that includes an IP address of the browser client.

17. An apparatus as recited in Claim 14, wherein the service request comprises an HTML POST form that includes an IP address of the browser client.

18. A computer-readable medium carrying one or more sequences of instructions for securely communicating a network address of a client that issues service requests to a first server that proxies the service requests for a second server, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

receiving a network address of the client;

determining whether a first network address of the first server is equal to a second network address of the second server; and

sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

19. A computer-readable medium as recited in Claim 18, wherein each of the service requests of the browser client comprises a key value comprising an IP address of the client and a random value.

20. A computer-readable medium as recited in Claim 18, wherein each of the service requests of the browser client comprises a Universal Resource Locator (URL) that includes an IP address of the browser client.

21. A computer-readable medium as recited in Claim 18, wherein each of the service requests of the browser client comprises an HTML POST form that includes an IP address of the browser client.

22. A data communications apparatus that securely communicates a service request that is received from a client, comprising:

a first server that proxies the service request for a second server comprising a network interface to a network that includes the first server and the second server;

a processor in the first server;

a storage device in the first server comprising one or more sequences of stored instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving a network address of the client;

determining whether a first network address of the first server is equal to a second network address of the second server; and

sending the network address of the client from the first server to the second server in a secure request message only when the first network address of the first server is equal to the second network address of the second server.

23. An apparatus as recited in Claim 22, wherein the service request comprises a key value comprising an IP address of the client and a random value.

24. An apparatus as recited in Claim 22, wherein the service request comprises a Universal Resource Locator (URL) that includes an IP address of the browser client.

25. An apparatus as recited in Claim 22, wherein the service request comprises an HTML POST form that includes an IP address of the browser client.